(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
21 décembre 2000 (21.12.2000)

PCT

(10) Numéro de publication internationale
WO 00/78009 A2

(51) Classification internationale des brevets[7]: H04L 29/06

(21) Numéro de la demande internationale:
PCT/FR00/01681

(22) Date de dépôt international: 16 juin 2000 (16.06.2000)

(25) Langue de dépôt: français

(26) Langue de publication: français

(30) Données relatives à la priorité:
99/07613 16 juin 1999 (16.06.1999) FR

(71) Déposants et
(72) Inventeurs: **LENOIR, Olivier** [FR/FR]; 10, rue des Fleurs, F-78180 Montigny le Bretonneux (FR). **COUR, Jean-Michel** [FR/FR]; 2, allée Galilée, F-91400 Orsay (FR).

(74) Mandataires: **PONTET, Bernard** etc.; Pontet Allano & Associés S.E.L.A.R.L., Parc-Club Orsay-Université, 25, rue Jean-Rostand, F-91893 Orsay Cedex (FR).

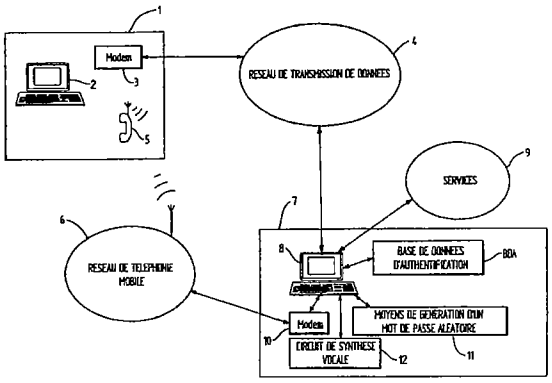
(81) États désignés *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) États désignés *(régional)*: brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), brevet eurasien

[Suite sur la page suivante]

(54) Title: METHOD AND SYSTEM FOR SECURELY ACCESSING A COMPUTER SERVER

(54) Titre: PROCEDE ET SYSTEME D'ACCES SECURISE A UN SERVEUR INFORMATIQUE



4 ... DATA TRANSMISSION NETWORK
6 ... MOBILE TELEPHONE NETWORK
11 .. MEANS GENERATING RANDOM PASSWORD
12 .. SPEECH SYNTHESIS CIRCUIT
BDA AUTHENTICATING DATABASE

(57) Abstract: The invention concerns a method for making secure the access to a computer server from a client site via at least a first communication network, said server comprising means for managing a protocol authenticating a user of a client site, comprising a reception sequence and processing of identification data of a user of a client site, and a sequence for transmitting a message from the server site to a communication equipment held by the user of the client site via a second communication network. The transmitted message is a voice message to be processed directly by said user to generate an authenticating password designed to be transmitted to said server site via one or the other of the first or second communication networks. The invention provides the advantage of enhancing security of authenticating protocols, particularly existing ones, at lower costs.

(57) Abrégé: Procédé de sécurisation d'accès à un serveur informatique depuis un site client via au moins un premier réseau de communication, ce serveur comprenant des moyens pour gérer un protocole d'authentification d'un utilisateur du site client, comprenant une séquence de réception et le traitement de données d'identification d'un utilisateur du site client, et une séquence

[Suite sur la page suivante]

WO 00/78009 A2

(AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Publiée:

— *Sans rapport de recherche internationale, sera republiée dès réception de ce rapport.*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

de transmission d'un message depuis le site serveur vers un équipement de communication détenu par l'utilisateur du site client via un second réseau de communication. Le message transmis est un message vocal destiné à être traité directement par ledit utilisateur pour générer un mot de passe d'authentification prévu pour être transmis audit site serveur via l'un ou l'autre des premier ou second réseaux de communication. Avantage: renforcement à moindre coût du niveau de sécurisation des protocoles d'authentification notamment existants.

"Procédé et système d'accès sécurisé à un serveur informatique"

La présente invention concerne un procédé permettant d'augmenter le niveau de sécurisation du protocole d'authentification du demandeur d'accès à un serveur informatique. Elle concerne également un système d'accès sécurisé mettant en œuvre ce procédé.

Un demandeur d'accès ou client utilise en pratique un ordinateur individuel ou un poste de travail muni de moyens de connexion à un réseau de communication, par exemple le réseau Internet.

Un serveur informatique est constitué d'un ordinateur muni de moyens de connexion au même réseau. Il sert à mettre en relation le client avec divers services tels que des bases de données.

Une procédure d'accès à un serveur pour un client se déroule classiquement en trois phases :

- l'accès au site serveur via l'établissement d'une connexion (par exemple TCP/IP), via un réseau généraliste ou privé de transmission de données (par exemple Internet) ;
- l'entrée d'une identification ; et
- l'entrée d'un mot de passe client.

L'accès est refusé si le couple [identification / mot de passe client] n'est pas conforme aux informations stockées dans une base de données dite d'"authentification " gérée par le serveur lui-même ou par un serveur intermédiaire adapté.

Les procédures connues présentent un certain nombre de faiblesses vis-à-vis de malveillances, telles que le vol des couples [code d'identification / mot de passe] via un logiciel de recherche automatique de mot de passe ou une complicité du côté " serveur " permettant de connaître le contenu de la base de données d'authentification.

Diverses solutions sont connues pour renforcer la sécurisation de l'accès :

- côté serveur un dispositif auxiliaire permettant la génération de mots de passe aléatoires et/ou cryptés, mais nécessitant la possession par le client d'un appareil synchronisé avec le serveur, générant un mot de passe pseudo-aléatoire et de courte durée de vie en fonction de la date et de l'heure ;
- la dotation des ordinateurs individuels d'un périphérique lecteur d'une carte électronique (" carte à puce "), sécurisant l'accès selon un protocole similaire à celui utilisé pour les cartes bancaires ; le client doit donc disposer d'une telle carte et d'un périphérique spécial sur le terminal à partir duquel il se connecte au réseau ;
- l'identification de la machine du client par un code d'identification tel que celui intégré par le constructeur sur ses microprocesseurs ; l'accès est sécurisé par identification du ou des composants connus du serveur ; l'inconvénient est qu'en dehors des machines dûment répertoriées, le client ne peut effectuer aucun accès.

Par ailleurs, les systèmes de cryptage connus, tels que l'algorithme RSA, nécessitent des puissances de calcul importantes pour obtenir un bon niveau de sécurité.

On connaît par le document WO9731306 un procédé pour fournir à un client des données d'authentification au moyen de services de transmission de message SMS sur son téléphone portable. via un réseau de téléphonie mobile.

Le document US5668876 divulgue un procédé pour authentifier un utilisateur d'un site fournisseur de service électronique connecté sur un réseau de communication, cet utilisateur détenant un téléphone portable. Ce procédé d'authentification comprend :

- une étape de transmission d'un code de demande sur un second réseau de communication, par exemple un réseau de téléphonie

mobile, ce code étant reçu sur une unité personnelle de l'utilisateur requérant,

- une étape de génération, au sein de l'unité personnelle de l'utilisateur, d'un code de réponse, fondée sur un algorithme ayant comme variables d'entrée le code de demande reçu et une donnée entrée par l'utilisateur,
- une étape de génération, au sein de l'unité personnelle, d'un code de sortie comprenant le code de réponse, ce code de sortie étant alors soit transmis à partir de l'unité personnelle vers le centre d'authentification, soit entré sur un terminal de l'utilisateur relié au premier réseau de communication,
- une étape de comparaison au sein du centre d'authentification entre le code de réponse reçu et le code de réponse attendu, et
- une étape pour permettre l'accès au service électronique en cas de comparaison satisfaite.

Les procédés de sécurisation ou d'authentification précités présentent l'inconvénient de nécessiter une coopération active d'un opérateur de téléphonie mobile et parfois une adaptation des équipements de communication mobile mis en œuvre dans ces procédés.

La présente invention a pour objet de proposer une autre solution qui ne nécessite pas l'intervention active d'un opérateur de téléphonie mobile et qui soit très fiable, très souple et peu coûteuse.

Elle propose un procédé d'accès sécurisé à un serveur informatique depuis un site client via au moins un premier réseau de communication, ce serveur comprenant des moyens pour gérer un protocole d'authentification d'un utilisateur du site client, comprenant une séquence de réception et le traitement de données d'identification d'un utilisateur du site client, et une séquence de transmission d'un message depuis le site serveur vers un équipement de communication

détenu par l'utilisateur du site client via un second réseau de communication.

Suivant l'invention, ce message transmis est un message vocal destiné à être traité directement par ledit utilisateur pour générer un mot de passe d'authentification prévu pour être transmis audit site serveur via l'un ou l'autre desdits premiers ou second réseaux de communication.

L'idée à la base de la présente invention est donc de faire intervenir dans le protocole d'authentification un téléphone mobile dans sa fonction de transmission vocale et non de transmission d'informations numériques ou de messages courts, le site serveur étant muni de moyens lui permettant d'appeler le téléphone mobile et de lui transmettre un message vocal.

Le premier réseau de communication peut être le réseau Internet et plus généralement tout réseau de communication filaire ou non filaire, par exemple un réseau de communication mobile.

Le second réseau de communication mis en œuvre dans le procédé de sécurisation selon l'invention est de préférence un réseau de communication mobile, mais pourrait être un réseau de communication fixe capable de communiquer avec des équipements de communication mobile.

Le procédé selon l'invention n'exige du côté du site client aucun dispositif informatique spécial d'identification, intégré ou périphérique. Il requiert la possession d'un téléphone mobile ordinaire, appareil qui tend à se généraliser parmi les professionnels et les particuliers. Le coût d'équipement côté serveur reste également modeste puisque notamment un modem standard du type comportant une unité de synthèse vocale peut être utilisé pour réaliser la connexion avec le réseau de téléphonie mobile.

Un autre avantage selon l'invention réside dans le fait que ni le poste serveur, ni le poste client ne nécessitent de puissances de calcul

importantes comparées aux systèmes de cryptage de l'état de la technique, d'où une forte réduction des coûts pour un système selon l'invention. On peut également prévoir une réduction des coûts de déploiement et surtout une absence de surcoût lors d'un changement des procédures par rapports aux solutions de sécurisation à base de matériel.

Il est à noter que la sécurisation apportée par le système selon l'invention est renforcée par la procédure d'identification du téléphone mobile lui-même par son réseau d'abonnement. Cette procédure met en oeuvre dans le cas de la norme GSM un composant électronique spécifique (carte SIM) branché sur l'appareil, et la possibilité pour le client d'avoir un mot de passe modifiable (code PIN) qui doit être saisi lors de la mise en marche du téléphone.

En cas de vol du téléphone mobile ou du composant SIM, celui-ci peut instantanément être mis hors service pour l'ensemble des réseaux GSM sur un simple appel au fournisseur d'abonnement du téléphone mobile. On pourra prévoir également que suivant une déclaration de vol, l'accès au réseau sera automatiquement fermé.

Le procédé selon l'invention permet de réutiliser les procédures existantes en ajoutant un niveau de sécurité. Il peut s'appliquer en complément de n'importe quel logiciel d'accès.

Ainsi, la donnée d'identification demandée au client peut être le couple [code d'identification / mot de passe client] (ID/MPC) du protocole d'authentification connu de l'état de la technique, de sorte que la connaissance directe ou indirecte de ce couple ne sera plus suffisante en soi pour obtenir l'accès au serveur.

Dans une première variante de réalisation, le procédé selon l'invention comprend les étapes consistant à :

- demander au site client des données d'identification via le premier réseau de communication ;

- traiter lesdites données et rechercher dans une base de données d'authentification un numéro d'appel d'un équipement de communication mobile détenu par l'utilisateur du site client ;
- appeler ledit équipement de communication mobile via au moins un second réseau de communication ;
- après établissement d'une communication avec ledit équipement de communication mobile, générer un mot de passe aléatoire ou pseudo-aléatoire;
- émettre un message vocal comprenant ledit mot de passe aléatoire via le second réseau de communication;
- demander à l'utilisateur de fournir, à partir du site client via le premier réseau de communication, un mot de passe d'authentification dérivé dudit mot de passe aléatoire ou pseudo-aléatoire ; et
- authentifier ledit mot de passe d'authentification.

Le mot de passe d'authentification peut par exemple correspondre au mot de passe aléatoire ou pseudo-aléatoire généré par le serveur et communiqué via l'équipement de communication mobile.

Mais on peut aussi prévoir que le mot de passe d'authentification sera constitué par le mot de passe aléatoire ou pseudo-aléatoire généré par le serveur et communiqué via l'équipement de communication mobile, auquel est appliquée une clé connue du client utilisateur et comprise dans la base de donnée d'authentification du serveur, l'étape d'authentification comportant une étape de conversion dudit mot de passe d'authentification en mot de passe aléatoire ou pseudo-aléatoire par application de ladite clé.

La clé peut être une constante connue et personnelle par exemple ajoutée ou retranchée pour obtenir le mot de passe serveur. Il peut s'agir aussi d'une opération de logique, comme une permutation.

Les données d'identification demandées au client peuvent consister en un couple [code d'identification / mot de passe client].

L'étape qui consiste à demander au client le mot de passe d'authentification se déroule de préférence pendant une durée prédéterminée au delà de laquelle l'authentification est refusée.

Dans une autre variante de réalisation du procédé selon l'invention, ce procédé comprend les étapes côté site serveur consistant à :

- demander au site client des données d'identification via le premier réseau de communication;
- traiter lesdites données et rechercher dans une base de données d'authentification un numéro d'appel d'un équipement de communication mobile détenu par l'utilisateur du site client ;
- appeler ledit équipement de communication mobile via au moins un second réseau de communication ;
- en cas d'obtention de la communication avec ledit équipement de communication mobile, émettre un message vocal requérant l'envoi par l'utilisateur d'une clé de cryptage ;
- recevoir et reconnaître la clé de cryptage transmise par le client via des touches de l'équipement de communication mobile;
- décrypter à l'aide de ladite clé de cryptage un mot de passe d'authentification transmis par le client via le premier réseau de communication, ce mot de passe d'authentification résultant d'un cryptage d'un mot de passe client réalisé sur le site client au moyen de la clé de cryptage ; et
- authentifier le mot de passe client résultant du décryptage du mot de passe d'authentification.

On peut également prévoir de remonter via le second réseau de communication mobile des informations d'accès résultant du message vocal transmis par le serveur via ce second réseau et le réaliser de nombreuses façons. On peut par exemple prévoir le processus suivant :

Un message vocal émis par le serveur est reçu via le second réseau de communication par un client utilisateur sur son téléphone portable, en réponse à une requête transmise au serveur via le premier réseau de communication à partir d'un terminal connecté à ce réseau. Ce message vocal indique par exemple un élément d'information à traiter sur le terminal.

Le client utilisateur effectue alors un traitement prédéterminé (par exemple, une translation ou toute autre modification simple ou complexe) à l'élément d'information indiqué et le frappe ensuite sur le clavier de son téléphone portable.

Ce mode spécifique de mise en œuvre du procédé de sécurisation selon l'invention est particulièrement adapté aux terminaux disposants de moyens de saisie rudimentaires tels que les terminaux de paiement électronique.

Suivant un autre aspect de l'invention, il est proposé un système de sécurisation d'accès à un serveur informatique depuis un site client via au moins un premier réseau de communication, mettant en œuvre le procédé selon l'invention, ce système comprenant sur le site serveur des moyens pour gérer un protocole d'authentification d'un utilisateur du site client, des moyens pour recevoir et traiter des données d'identification d'un utilisateur du site client, et des moyens pour générer et pour transmettre un message depuis le site serveur vers un équipement de communication détenu par l'utilisateur du site client via un second réseau de communication, caractérisé en ce que ce système est agencé pour transmettre via le second réseau de communication un message vocal destiné à être traité directement par ledit utilisateur pour générer un mot de passe d'authentification prévu pour être transmis audit site serveur via ledit premier réseau de communication.

Ce système peut en outre avantageusement comprendre, dans une première variante de réalisation :

- des moyens pour rechercher, en réponse à une réception de données d'identification en provenance d'un site client requérant un accès, dans une base de données d'authentification un numéro d'appel d'un équipement de communication mobile détenu par l'utilisateur du site client ;

- des moyens pour appeler ledit équipement de communication mobile via au moins un second réseau de communication ;

- des moyens pour générer un mot de passe aléatoire ou pseudo-aléatoire, et

- des moyens pour authentifier un mot de passe d'authentification en provenance du site client via le premier réseau de communication,

caractérisé en ce qu'il comprend en outre :

- des moyens pour émettre un message vocal comprenant ledit mot de passe aléatoire via le second réseau de communication, et

- des moyens pour requérir de l'utilisateur dudit site client une fourniture, via le premier réseau de communication, d'un mot de passe d'authentification dérivé dudit mot de passe aléatoire ou pseudo-aléatoire.

Dans une seconde variante de réalisation, le système selon l'invention peut avantageusement comprendre :

- des moyens pour demander au site client des données d'identification via le premier réseau de communication;

- des moyens pour traiter lesdites données et rechercher dans une base de données d'authentification un numéro d'appel d'un équipement de communication mobile détenu par l'utilisateur du site client ;

- des moyens pour appeler ledit équipement de communication mobile via au moins un second réseau de communication ;

- des moyens pour émettre un message vocal requérant l'envoi par l'utilisateur d'une clé de cryptage ;

- des moyens pour recevoir et reconnaître la clé de cryptage transmise par le client via des touches de l'équipement de communication mobile;

- des moyens pour décrypter à l'aide de ladite clé de cryptage un mot de passe d'authentification transmis par le client via le premier réseau de communication, ce mot de passe d'authentification résultant d'un cryptage d'un mot de passe client réalisé sur le site client au moyen de la clé de cryptage ; et

- des moyens pour authentifier le mot de passe client résultant du décryptage du mot de passe d'authentification.

On pourra également renforcer la sécurisation du procédé selon l'invention, en prévoyant la désactivation automatique de l'accès au serveur dès qu'un nombre prédéterminé de tentatives a échoué à l'une quelconque des étapes de saisie, et la possibilité de demander la désactivation immédiate du téléphone auprès du fournisseur de téléphonie mobile.

Suivant encore un autre aspect de l'invention, il est proposé une application du procédé de sécurisation selon l'invention dans un système d'authentification d'œuvres numériques comportant des sites tierces parties de datation, d'authentification et d'archivage connectés à un premier réseau de communication, caractérisée en ce que chaque site tierce partie comprend localement des moyens logiciels prévus (i) pour transmettre sous forme vocale à un site client sollicitant une opération d'authentification des données de sécurisation via un équipement de communication mobile associé audit site client et connecté à un second réseau de communication, et (ii) pour recevoir dudit site client via le premier réseau de communication un mot de passe d'authentification résultant desdites données de sécurisation.

La présente invention sera mieux comprise et d'autres avantages apparaîtront à la lumière de la description qui va suivre de deux exemples de réalisation du système et des procédés associés selon l'invention, description faite en référence aux dessins annexés sur lesquels :

- la figure 1 est un schéma synoptique du premier exemple de réalisation du système selon l'invention ;

- la figure 2 est un organigramme du procédé d'authentification exécuté par le serveur mettant en oeuvre le système de la figure 1 ;

- la figure 3 montre schématiquement une page écran générée par le serveur et utilisée par le client pour la transaction d'authentification du procédé de la figure 2 ;

- la figure 4 est un schéma synoptique du second exemple de réalisation du système selon l'invention ;

- la figure 5 est un organigramme du procédé d'authentification exécuté par le serveur mettant en oeuvre le système de la figure 4 ;

- la figure 6 montre schématiquement une page écran générée par le serveur et utilisée par le client pour la transaction d'authentification du procédé de la figure 5 ; et

- la figure 7 est un schéma synoptique illustrant une application du procédé de sécurisation selon l'invention pour la protection juridique d'œuvres numériques.

Comme illustré schématiquement à la figure 1, un premier exemple de réalisation du système selon l'invention comprend :

- sur un site client 1, un ordinateur individuel 2 équipé d'un modem 3 pour accéder à un réseau de transmission de données 4 et un téléphone mobile 5 personnel, abonné à un réseau de téléphonie mobile 6, par exemple au standard GSM ; et

- sur un site serveur 7, un serveur constitué d'un ordinateur 8 sur lequel est chargé un logiciel adapté à gérer le procédé d'accès du client aux services 9 du serveur selon l'invention, notamment le protocole d'authentification du client ; l'ordinateur est équipé d'un modem 10 lui permettant d'établir une liaison avec le réseau de téléphonie mobile 6 et d'appeler un numéro de téléphone, de moyens 11 de génération d'un mot de passe aléatoire ou pseudo-aléatoire MPA, et d'un circuit de synthèse vocale 12 lui permettant de

communiquer au téléphone mobile 5 un message comprenant le mot de passe MPA généré aléatoirement nécessaire au protocole d'authentification. L'ordinateur 8 est relié à une base de données d'authentification BDA comprenant pour chaque client répertorié un triplet [code d'identification ID / mot de passe client MPC/numéro de téléphone mobile personnel associé].

Le procédé d'accès sécurisé se déroule de la manière suivante.

Le client sur le site client 1 demande l'accès au serveur. La liaison entre le site client 1 et le site serveur 7 via le réseau de transmission de données 4 se fait de manière classique et connue en soi par l'intermédiaire du modem 3 du site client 1, du réseau téléphonique commuté, d'un fournisseur d'accès au réseau généraliste Internet et d'Internet.

En retour, le serveur affiche sur l'ordinateur individuel 2 une page écran 15, représentée sur la figure 3, comprenant trois champs de saisie : les deux premiers champs 16 et 17 correspondent au couple classique [code d'identification ID et mot de passe client MPC], le troisième champ 18 correspond à un mot de passe d'authentification MPAUT qui est dérivé du mot de passe aléatoire ou pseudo-aléatoire MPA qui sera communiqué par le serveur au site client 1 via le téléphone mobile 5. Ce mot de passe d'authentification MPAUT correspond ici au mot de passe aléatoire ou pseudo-aléatoire MPA généré par le serveur.

Dans un premier temps, le client saisit son couple [code d'identification-mot de passe client] (ID/MPC) qui est déjà sécurisé par n'importe quel processus connu à partir de la base de données d'authentification BDA.

En se référant à l'organigramme de la figure 2, les étapes suivantes du protocole, spécifiques à la présente invention, ne seront exécutées par le serveur qu'à la condition préalable que l'étape de

contrôle identification / mot de passe client à l'étape 20 soit couronnée de succès.

Si tel est le cas, l'étape suivante 21 consiste à composer le numéro du téléphone mobile identifié grâce à la base de données d'authentification BDA à l'aide du modem 10. A l'étape suivante 22, si la communication téléphonique avec le téléphone mobile est obtenue (par exemple par l'indication du " décrochage " par le modem 10 du site serveur), le serveur génère un mot de passe aléatoire MPA et émet grâce à son circuit de synthèse vocale ce mot de passe MPA généré vers le téléphone mobile 5. L'étape suivante 23 correspond à une étape d'attente de la saisie du mot de passe d'authentification MPAUT par le client au niveau du site client pendant une durée limitée prédéterminée (étape 24). Si à l'étape 25, le mot de passe MPAUT saisi est conforme, l'authentification est confirmée et le client peut accéder aux services 9 du serveur.

L'échec de l'authentification intervient donc dans les circonstances suivantes :

- échec de l'authentification classique du couple [ID /MPC] ;
- non-obtention de la communication avec le téléphone mobile ;
- mauvaise ou absence d'entrée du second mot de passe MPAUT dans le délai prédéterminé.

Des variantes de réalisation sont possibles, notamment concernant le mot de passe serveur dérivé du mot de passe aléatoire MPA qui peut être constitué dudit mot de passe aléatoire MPA auquel est ajoutée une clé arithmétique ou logique personnelle au client et comprise dans la base de données d'authentification BDA dans un champ supplémentaire à ceux déjà prévus pour le code d'identification ID, le mot de passe client MPC et le numéro de téléphone mobile. Le serveur sera équipé de moyens lui permettant de recalculer le mot de passe généré MPA pour procéder à l'étape d'authentification.

Les figures 4 à 6 concernent un autre mode de réalisation du système selon l'invention se différenciant par le fait que le site client 1 est équipé en outre de moyens de cryptage 30 qui sont adaptés à crypter le mot de passe client MPC une fois celui-ci saisi par le client avant de l'envoyer via le réseau 4 de transmission de données au site serveur 7. Du côté du site serveur, celui se différencie par des moyens de reconnaissance 31 d'un signal envoyé par le client via les touches de son téléphone mobile personnel 5 et des moyens de décryptage 32 adaptés à décrypter le mot de passe client MPC selon une clé de cryptage qui est transmise par le client via les touches de son téléphone mobile. La base de données d'authentification BDA ne comporte ici que deux champs contenant l'un le code ID et l'autre le mot de passe client MPC. Le protocole d'authentification après décryptage correspond au protocole connu dans l'art antérieur.

Le procédé d'accès sécurisé utilisant ce système se déroule de la manière suivante.

En réponse à une demande d'accès de la part du client utilisant le site client 1, le serveur affiche sur l'ordinateur individuel 2 une page écran 35 représentée à la figure 6, ne comprenant par rapport au premier mode de réalisation que deux champs de saisie 36 et 37 qui correspondent au couple classique [code d'identification ID et mot de passe client MPC]. Immédiatement après la saisie du mot de passe client MPC, les moyens 30 cryptent le mot de passe client saisi selon une clé de cryptage connue seulement du client. Ce mot de passe client crypté correspond au mot de passe dit d'authentification du procédé selon l'invention.

En se référant à l'organigramme de la figure 5, les étapes du protocole d'authentification se déroulent de la manière suivante.

Dans un premier temps, à l'étape 40, le serveur, ayant reçu le mot de passe client crypté et le code ID, identifie le client à l'aide du code d'identification ID, puis à l'étape 41, il recherche dans la base de

données d'authentification BDA, le numéro de téléphone mobile. L'étape 42 suivante consiste à composer le numéro du téléphone mobile à l'aide du modem 10. Si à l'étape suivante 43 la communication avec le téléphone mobile est obtenue, le serveur émet grâce à son circuit de synthèse vocale 12 un message (étape 45) signalant qu'il attend de la part du client la clé de cryptage via les touches du téléphone mobile. L'étape 46 correspond à une étape d'attente de la saisie de cette clé pendant une durée limitée prédéterminée. L'étape suivante 47 consiste à authentifier le mot de passe MPAUT reçu via le réseau 4 par le décryptage de ce mot de passe avec la clé et l'authentification du mot de passe client obtenu, conformément au protocole d'authentification. Si le mot de passe client MPC est conforme (étape 48), l'authentification est confirmée et le client peut accéder aux services 9 offert par le serveur.

L'échec de l'authentification interviendra donc dans les circonstances suivantes :

- non-obtention de la communication avec le téléphone mobile ; et
- mauvaise ou absence d'entrée du mot de passe client MPC et de la clé de cryptage.

Le procédé de sécurisation selon l'invention peut trouver une application particulièrement intéressante lorsqu'il est mis en œuvre dans le cadre d'un système de protection juridique et d'authentification d'œuvres numériques représenté schématiquement en figure 7. Ce système, construit autour d'Internet et du web, comprend un premier site S1 procurant une fonction de tierce partie de datation, un second site S2 procurant une fonction de tierce partie d'authentification, et un troisième site S3 procurant une fonction de tierce partie d'archivage. Il peut en outre comporter, sans que cela soit pour autant indispensable, un site SP fournisseur de services d'authentification procurant une fonction de portail et d'aiguillage vers les différentes sites précités.

Chacune des sites tierces parties est équipé d'un logiciel implémentant le procédé de sécurisation selon l'invention. Lorsqu'un client auteur ou détenteur d'une œuvre numérique sollicite chacun des sites tierces parties S1, S2, S3, soit directement soit via le site portail fournisseur de services SP, le procédé de sécurisation selon l'invention est exécuté avec fourniture à ce client via un réseau d'un opérateur de téléphonie mobile d'un mot de passe MPA1, MPA2, MPA3, puis émission par le client via Internet d'un mot de passe d'authentification MPAU1, MPAU2, MPAU3 destiné au site tierce partie sollicité. On peut bien sûr prévoir que l'autorité judiciaire puisse directement accéder en cas de besoin aux informations et données stockées dans les différentes sites tierces parties pour le compte des clients utilisateurs de ce système d'authentification mettant en œuvre le procédé de sécurisation selon l'invention.

Bien sûr, l'invention n'est pas limitée aux exemples qui viennent d'être décrits et de nombreux aménagements peuvent être apportés à ces exemples sans sortir du cadre de l'invention. En particulier, le procédé de sécurisation selon l'invention peut aussi concerner les équipements mobiles d'accès à Internet utilisant la technologie WAP (Wired Access protocole). On pourra aussi prévoir que sur un même équipement mobile soient accessibles un premier réseau de communication mobile WAP procurant un accès à Internet et un second réseau de communication mobile procurant le vecteur de transmission des mots de passe transmis par un site mettant en œuvre le procédé de sécurisation selon l'invention.

Revendications

1. Procédé de sécurisation d'accès à un serveur informatique depuis un site client via au moins un premier réseau de communication, ce serveur comprenant des moyens pour gérer un protocole d'authentification d'un utilisateur du site client, comprenant une séquence de réception et le traitement de données d'identification d'un utilisateur du site client, et une séquence de transmission d'un message depuis le site serveur vers un équipement de communication détenu par l'utilisateur du site client via un second réseau de communication, caractérisé en ce que ce message transmis est un message vocal destiné à être traité directement par ledit utilisateur pour générer un mot de passe d'authentification prévu pour être transmis audit site serveur via l'un ou l'autre desdits premier ou second réseaux de communication.

2. Procédé de sécurisation selon la revendication 1, caractérisé en ce qu'il comprend les étapes consistant à :

- demander au site client des données d'identification (ID,MPC) via le premier réseau de communication (4) ;
- traiter lesdites données (ID,MPC) et rechercher dans une base de données d'authentification (BDA) un numéro d'appel d'un équipement de communication mobile détenu par l'utilisateur du site client ;
- appeler ledit équipement de communication mobile via au moins un second réseau de communication ;
- après établissement d'une communication avec ledit équipement de communication mobile, générer un mot de passe aléatoire ou pseudo-aléatoire (MPA) ;

- émettre un message vocal comprenant ledit mot de passe aléatoire (MPA) via le second réseau de communication (6) ;
- demander à l'utilisateur de fournir, à partir du site client via le premier réseau de communication (4), un mot de passe d'authentification (MPAUT) dérivé dudit mot de passe aléatoire ou pseudo-aléatoire (MPA) ; et
- authentifier ledit mot de passe d'authentification (MPAUT).

3. Procédé selon la revendication 2, caractérisé en ce que le mot de passe d'authentification (MPAUT) correspond au mot de passe aléatoire ou pseudo-aléatoire (MPA) généré par le serveur et communiqué via l'équipement de communication mobile.

4. Procédé selon la revendication 2, caractérisé en ce que le mot de passe d'authentification (MPAUT) est constitué par le mot de passe aléatoire ou pseudo-aléatoire (MPA) généré par le serveur et communiqué via l'équipement de communication mobile, auquel est appliquée une clé connue du client utilisateur et comprise dans la base de donnée d'authentification du serveur (BDA), l'étape d'authentification comportant une étape de conversion dudit mot de passe d'authentification en mot de passe aléatoire ou pseudo-aléatoire (MPA) par application de ladite clé.

5. Procédé selon l'une des revendications précédentes, caractérisé en ce que les données d'identification demandées au client consistent en un couple [code d'identification / mot de passe client] (ID/MPC).

6. Procédé selon l'une des revendications précédentes, caractérisé en ce que l'étape qui consiste à demander au client le mot de passe d'authentification (MPAUT) se déroule pendant une durée prédéterminée au delà de laquelle l'authentification est refusée.

7. Procédé de sécurisation selon la revendication 1, caractérisé en ce qu'il comprend les étapes côté site serveur consistant à :

- demander au site client des données d'identification (ID,MPC) via le premier réseau de communication (4) ;

- traiter lesdites données (ID,MPC) et rechercher dans une base de données d'authentification (BDA) un numéro d'appel d'un équipement de communication mobile détenu par l'utilisateur du site client ;

- appeler ledit équipement de communication mobile via au moins un second réseau de communication ;

- en cas d'obtention de la communication avec ledit équipement de communication mobile, émettre un message vocal requérant l'envoi par l'utilisateur d'une clé de cryptage ;

- recevoir et reconnaître la clé de cryptage transmise par le client via des touches de l'équipement de communication mobile;

- décrypter à l'aide de ladite clé de cryptage un mot de passe d'authentification (MPAUT) transmis par le client via le premier réseau de communication, ce mot de passe d'authentification résultant d'un cryptage d'un mot de passe client réalisé sur le site client au moyen de la clé de cryptage ; et

- authentifier le mot de passe client (MPC) résultant du décryptage du mot de passe d'authentification.

8. Procédé selon la revendication 7, caractérisé en ce que l'étape de réception de la clé de cryptage se déroule pendant une durée prédéterminée au delà de laquelle l'authentification est refusée.

9. Système de sécurisation d'accès à un serveur informatique depuis un site client via au moins un premier réseau de communication, mettant en œuvre le procédé selon l'une quelconque des revendications précédentes, ce système comprenant sur le site serveur

des moyens pour gérer un protocole d'authentification d'un utilisateur du site client, des moyens pour recevoir et traiter des données d'identification d'un utilisateur du site client, et des moyens pour générer et pour transmettre un message depuis le site serveur vers un équipement de communication détenu par l'utilisateur du site client via un second réseau de communication, caractérisé en ce que ce système est agencé pour transmettre via le second réseau de communication un message vocal destiné à être traité directement par ledit utilisateur pour générer un mot de passe d'authentification prévu pour être transmis audit site serveur via ledit premier réseau de communication.

10. Système de sécurisation selon la revendication 9, comprenant en outre :

- des moyens pour rechercher, en réponse à une réception de données d'identification en provenance d'un site client requérant un accès, dans une base de données d'authentification (BDA) un numéro d'appel d'un équipement de communication mobile détenu par l'utilisateur du site client ;
- des moyens pour appeler ledit équipement de communication mobile via au moins un second réseau de communication ;
- des moyens pour générer un mot de passe aléatoire ou pseudo-aléatoire (MPA), et
- des moyens pour authentifier un mot de passe d'authentification en provenance du site client via le premier réseau de communication,

caractérisé en ce qu'il comprend en outre :

- des moyens pour émettre un message vocal comprenant ledit mot de passe aléatoire (MPA) via le second réseau de communication (6), et
- des moyens pour requérir de l'utilisateur dudit site client une fourniture, via le premier réseau de communication (4), d'un mot de passe d'authentification (MPAUT) dérivé dudit mot de passe aléatoire ou pseudo-aléatoire (MPA).

11. Système de sécurisation selon la revendication 9, comprenant :

- des moyens pour demander au site client des données d'identification (ID,MPC) via le premier réseau de communication (4) ;
- des moyens pour traiter lesdites données (ID,MPC) et rechercher dans une base de données d'authentification (BDA) un numéro d'appel d'un équipement de communication mobile détenu par l'utilisateur du site client ;
- des moyens pour appeler ledit équipement de communication mobile via au moins un second réseau de communication ;
- des moyens pour émettre un message vocal requérant l'envoi par l'utilisateur d'une clé de cryptage ;
- des moyens pour recevoir et reconnaître la clé de cryptage transmise par le client via des touches de l'équipement de communication mobile;
- des moyens pour décrypter à l'aide de ladite clé de cryptage un mot de passe d'authentification (MPAUT) transmis par le client via le premier réseau de communication, ce mot de passe d'authentification résultant d'un cryptage d'un mot de passe client réalisé sur le site client au moyen de la clé de cryptage ; et
- des moyens pour authentifier le mot de passe client (MPC) résultant du décryptage du mot de passe d'authentification.

12. Application du procédé de sécurisation selon l'une quelconque des revendications 1 à 8 dans un système d'authentification d'œuvres numériques comportant des sites tierces parties de datation, d'authentification et d'archivage connecté à un premier réseau de communication, caractérisée en ce que chaque site tierce partie comprend localement des moyens logiciels prévus (i) pour transmettre sous forme vocale à un site client sollicitant une opération d'authentification des données de sécurisation via un équipement de communication mobile associé audit site client et connecté à un

second réseau de communication, et (ii) pour recevoir dudit site client via le premier réseau de communication un mot de passe d'authentification résultant desdites données de sécurisation.

5

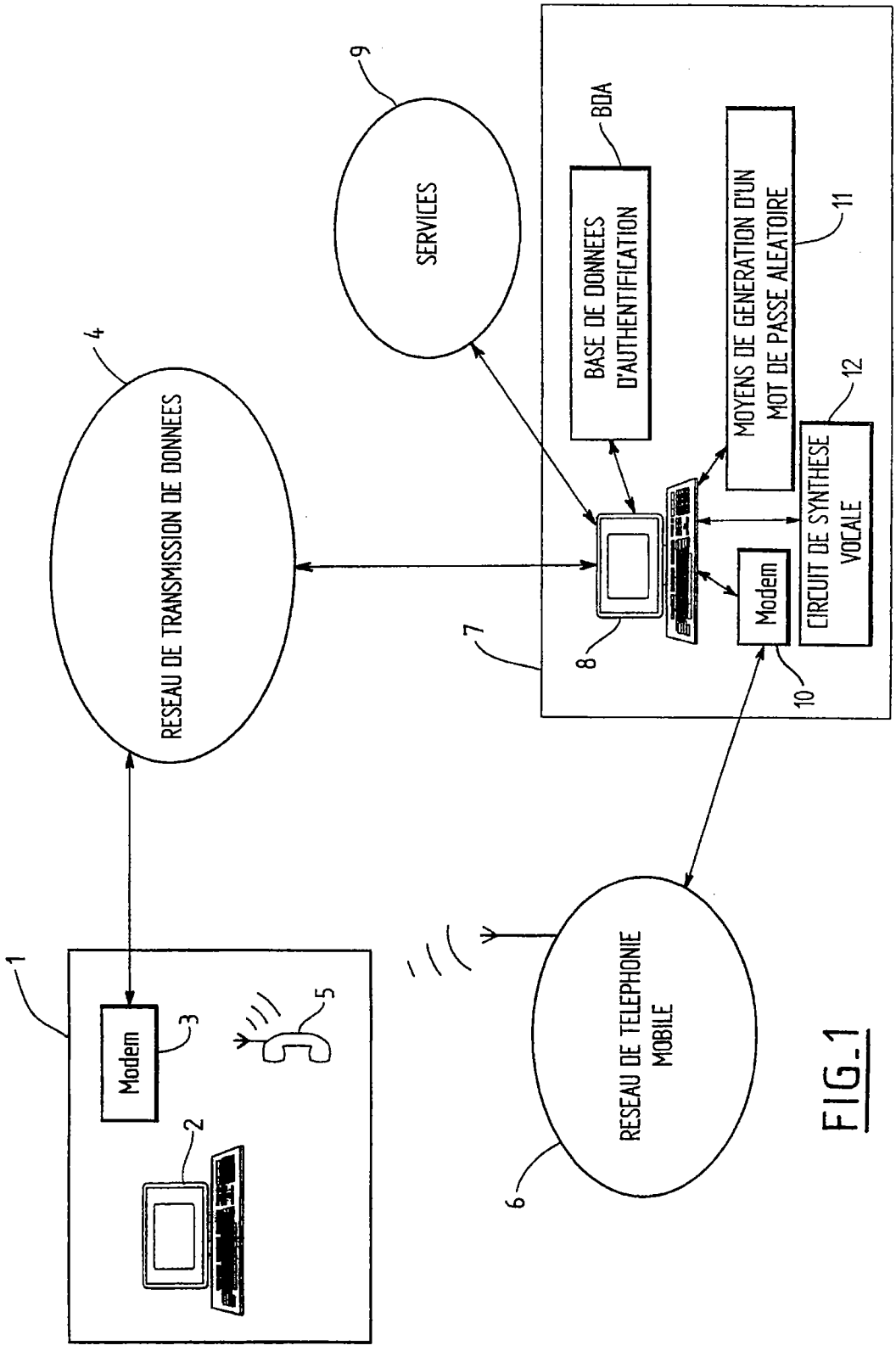
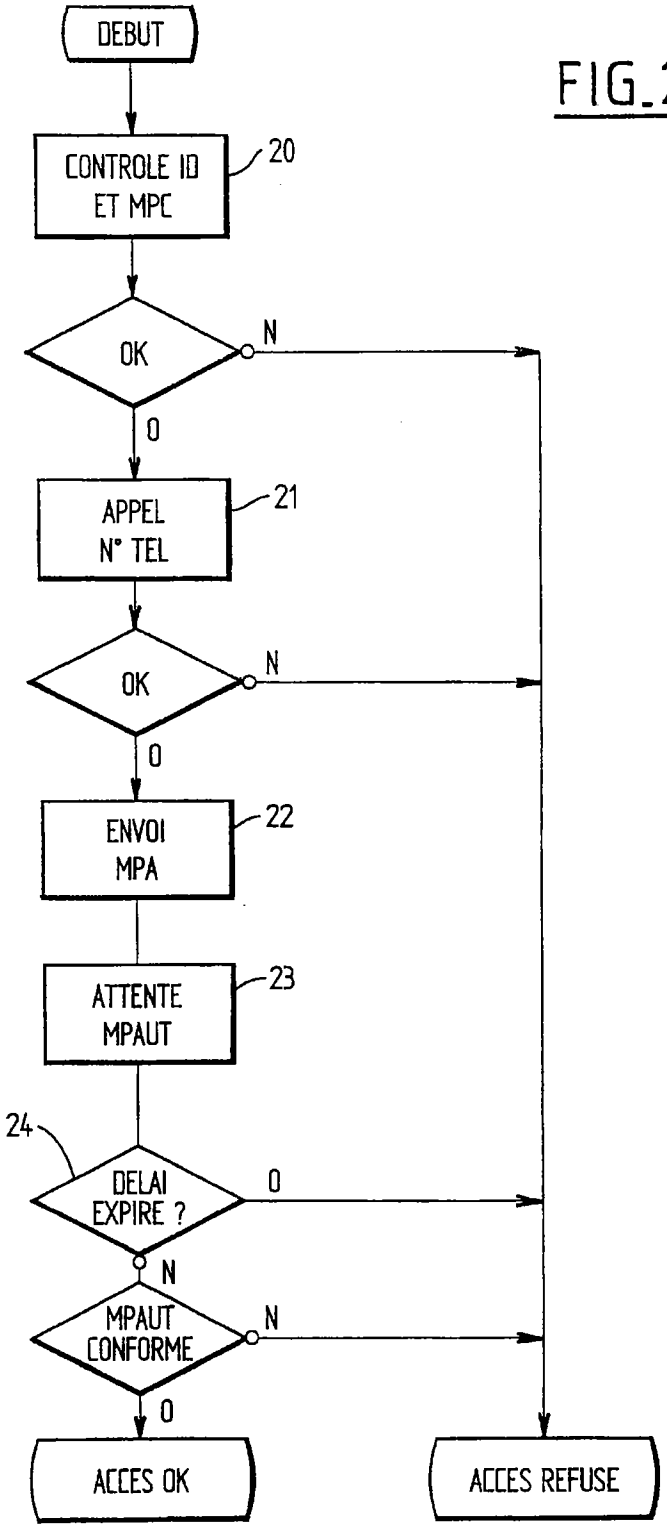

1
Modem
3
2
5
RESEAU DE TRANSMISSION DE DONNEES
4
SERVICES
9
BDA
BASE DE DONNEES D'AUTHENTIFICATION
MOYENS DE GENERATION D'UN MOT DE PASSE ALEATOIRE
11
12
CIRCUIT DE SYNTHESE VOCALE
Modem
10
8
7
RESEAU DE TELEPHONIE MOBILE
6

FIG.1

FIG_2


DEBUT
CONTROLE ID ET MPC
20
OK
N
O
APPEL N° TEL
21
OK
N
O
ENVOI MPA
22
ATTENTE MPAUT
23
24
DELAI EXPIRE ?
O
N
MPAUT CONFORME
N
O
ACCES OK
ACCES REFUSE

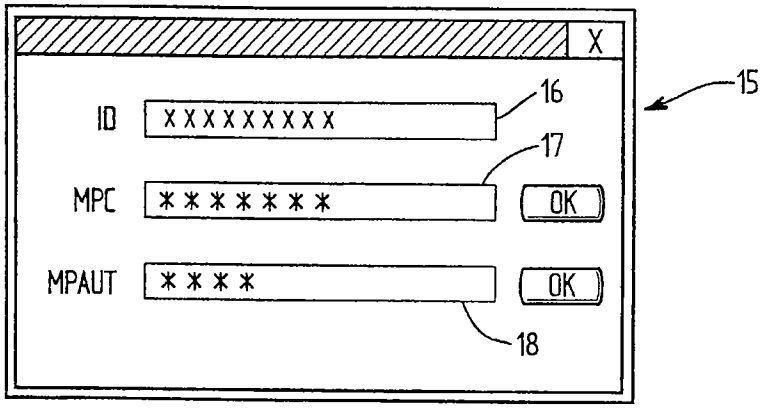

X
ID
XXXXXXXXX
16
15
17
MPC
****
OK
MPAUT
****
OK
18

FIG_3

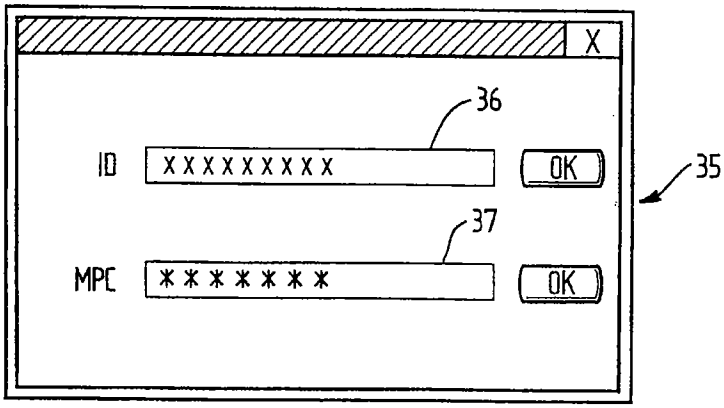

X
36
ID
XXXXXXXXX
OK
35
37
MPC
****
OK

FIG_6

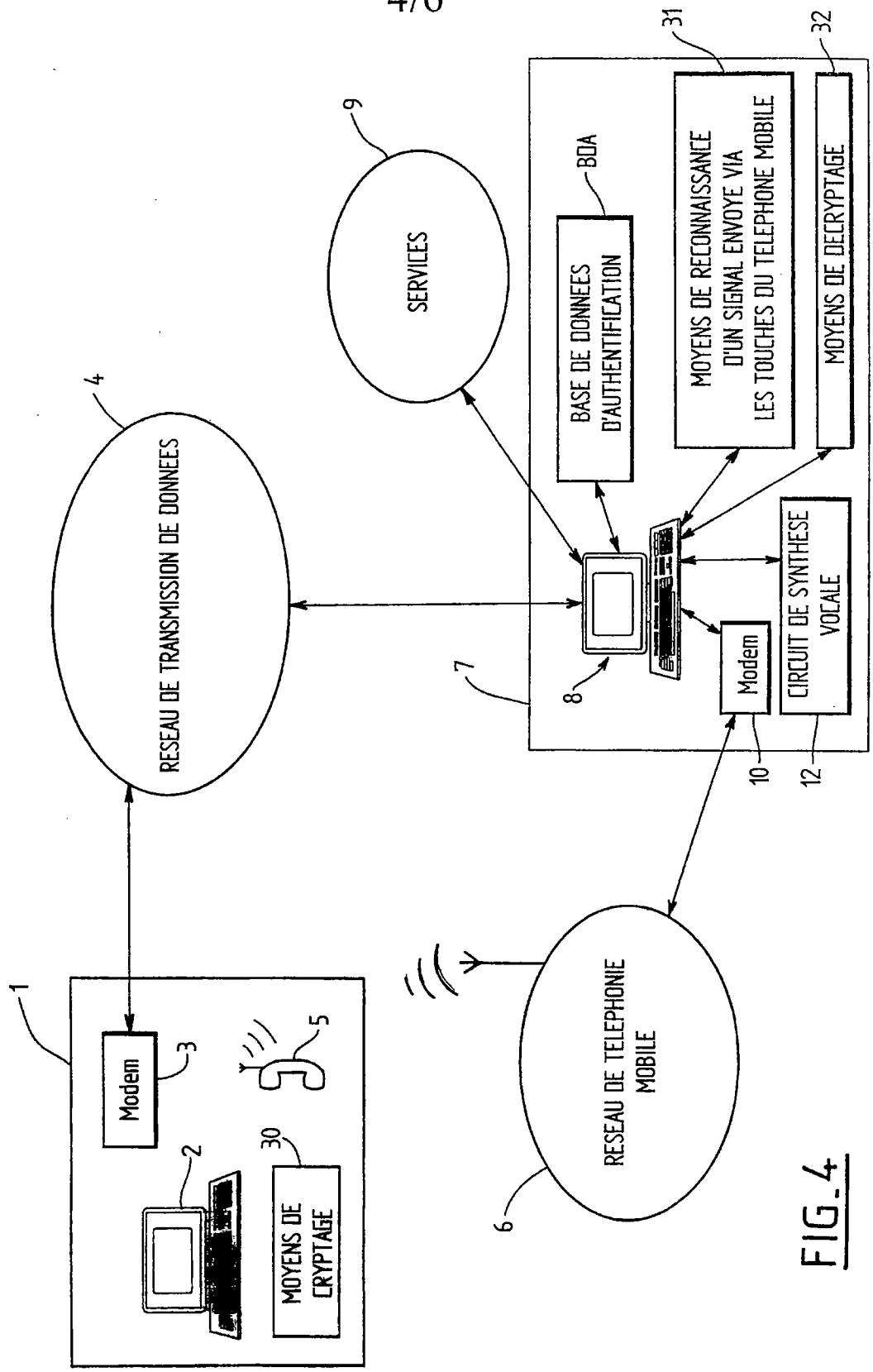

1
Modem
3
5
2
30
MOYENS DE CRYPTAGE
RESEAU DE TRANSMISSION DE DONNEES
4
SERVICES
9
BDA
BASE DE DONNEES D'AUTHENTIFICATION
31
MOYENS DE RECONNAISSANCE D'UN SIGNAL ENVOYE VIA LES TOUCHES DU TELEPHONE MOBILE
32
MOYENS DE DECRYPTAGE
7
8
Modem
10
CIRCUIT DE SYNTHESE VOCALE
12
RESEAU DE TELEPHONIE MOBILE
6

FIG_4

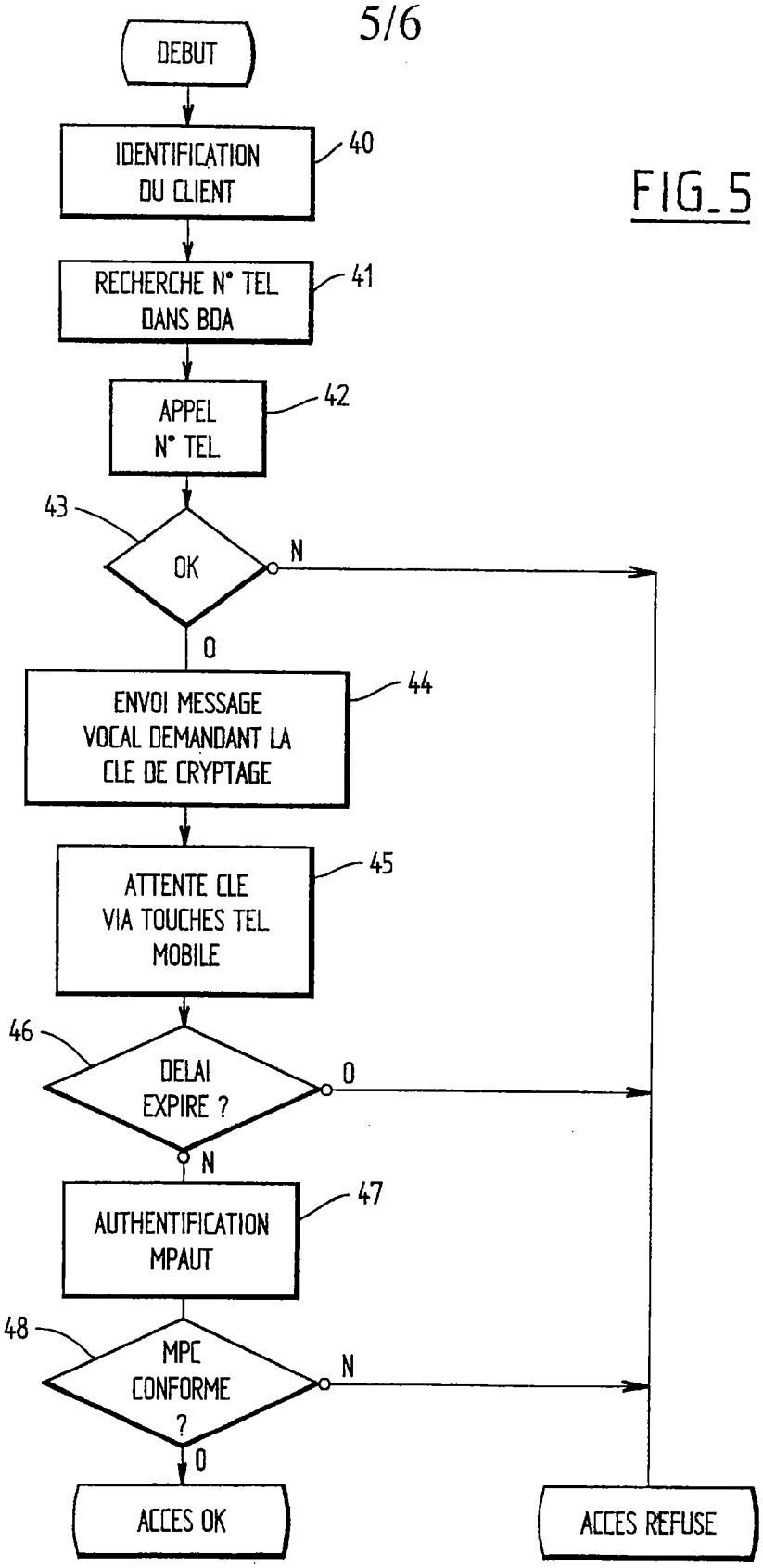

DEBUT
IDENTIFICATION DU CLIENT
40
RECHERCHE N° TEL DANS BDA
41
APPEL N° TEL
42
43
OK
N
O
ENVOI MESSAGE VOCAL DEMANDANT LA CLE DE CRYPTAGE
44
ATTENTE CLE VIA TOUCHES TEL MOBILE
45
46
DELAI EXPIRE ?
O
N
AUTHENTIFICATION MPAUT
47
48
MPC CONFORME ?
N
O
ACCES OK
ACCES REFUSE

FIG_5

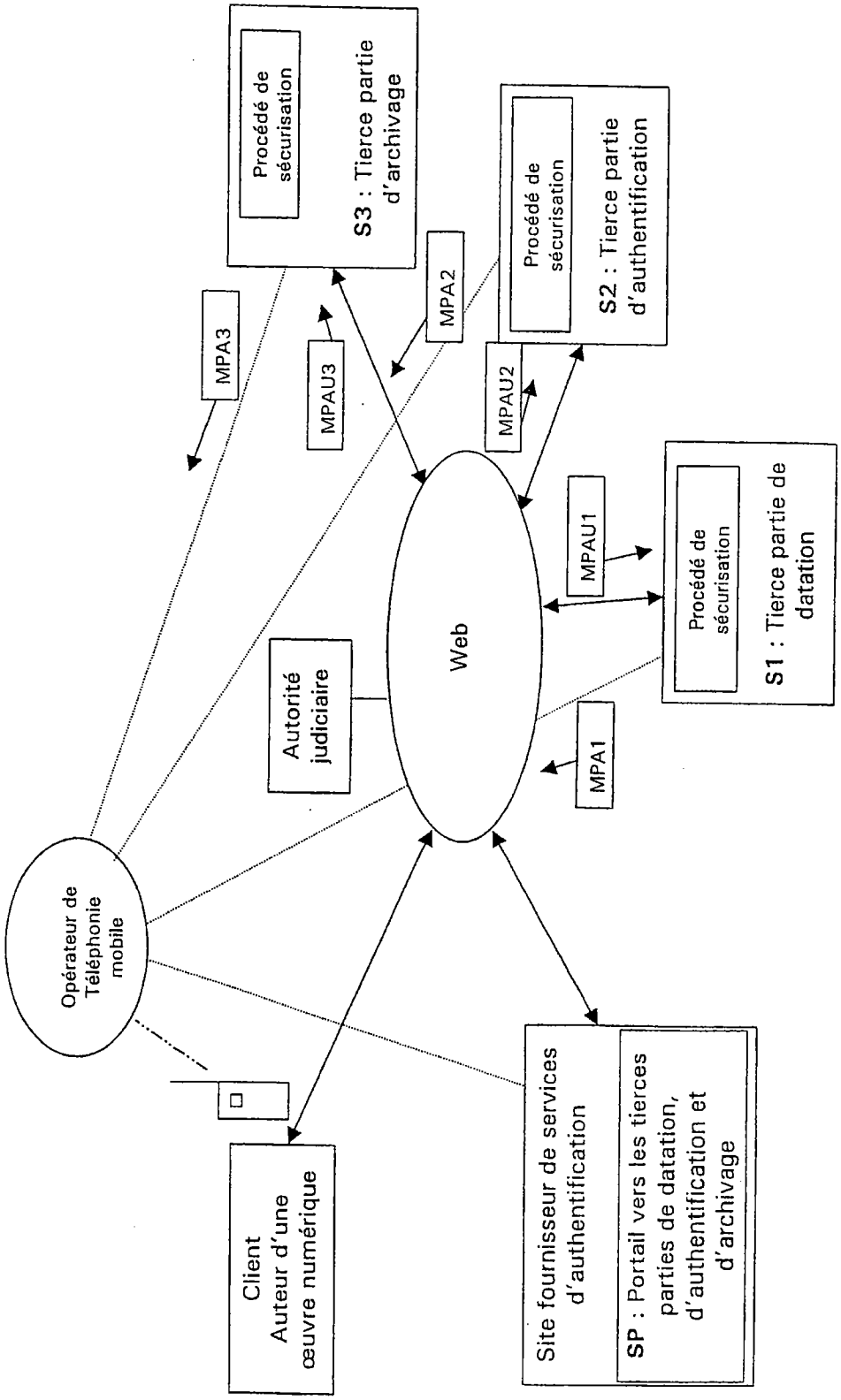

Procédé de sécurisation
S3 : Tierce partie d'archivage
Procédé de sécurisation
S2 : Tierce partie d'authentification
Procédé de sécurisation
S1 : Tierce partie de datation
MPA3
MPAU3
MPA2
MPAU2
MPAU1
MPA1
Web
Autorité judiciaire
Opérateur de Téléphonie mobile
Client Auteur d'une œuvre numérique
Site fournisseur de services d'authentification
SP : Portail vers les tierces parties de datation, d'authentification et d'archivage

FIG.7